Amendments to the claims (this listing replaces all prior versions):

1. (currently amended) A method comprising:

detecting [[a]] possible security ~~problem~~ problems at [[a]] client ~~location~~ locations;

transmitting notice of the possible security ~~problem~~ problems across a network in real time to a home location remotely located from the client ~~location~~ locations;

determining at the home location an anomaly based on at least the possible security ~~problem~~ problems ~~and on information sent to the home location from at least one other client location~~; ~~and~~

transmitting notice of the anomaly in real time to the client ~~location~~ locations at which the possible security ~~problem is~~ problems are detected; and

updating, in real time, firewalls protecting the client locations to account for the anomaly.

2. (original) The method of claim 1 further comprising transmitting notice of the anomaly in real time to other client locations that may communicate with the home location over the network.

3. (cancelled)

4. (original) The method of claim 1 further comprising inspecting a packet that arrives at the client location to detect the possible security problem.

5. (currently amended) The method of claim 1 in which the ~~network includes a~~ updating the firewalls comprises sending update information to the firewalls through virtual private ~~network~~ networks.

6. (original) The method of claim 1 in which the anomaly includes unauthorized access to the network.

7. (original) The method of claim 1 in which the anomaly includes unauthorized access of a resource accessible through the network.

8. (original) The method of claim 1 in which the anomaly includes unauthorized use of resources available through the network.

9. (currently amended) An article comprising:

a machine-readable medium which contains machine-executable instructions, the instructions causing a machine to:

detect [[a]] possible security ~~problem~~ problems at [[a]] client ~~location~~ locations;

transmit notice of the possible security ~~problem~~ problems across a network in real time to a home location remotely located from the client ~~location~~ locations;

determine at the home location an anomaly based on at least the possible security ~~problem~~ problems; ~~and on information sent to the home location from at least one other client location; and~~

transmit notice of the anomaly in real time to the client ~~location~~ locations at which the possible security ~~problem is~~ problems are detected; and

updating, in real time, firewalls protecting the client locations to account for the anomaly.

10. (original) The article of claim 9 further causing a machine to transmit notice of the anomaly in real time to other client locations that may communicate with the home location over the network

11. (cancelled)

12. (currently amended) The article of claim 9 further causing [[a]] the machine to inspect a packet that arrives at the client location to detect the possible security problem.

13. (currently amended) The article of claim 9 in which ~~the network includes a~~ updating the firewalls comprises sending update information to the firewalls through virtual private ~~network~~ networks.

14. (original) The article of claim 9 in which the anomaly includes unauthorized access to the network.

15. (original) The article of claim 9 in which the anomaly includes unauthorized access of a resource accessible through the network.

16. (original) The article of claim 9 in which the anomaly includes unauthorized use of resources available through the network.

17. (currently amended) A method comprising:

at a home location in a network, receiving from [[a]] at least two remote ~~client an indication~~ clients indications of [[a]] possible security ~~problem~~ problems at the ~~client~~ clients; ~~and~~

determining in real time at the home location an existence of an anomaly based on at least the ~~indication~~ indications of the possible security ~~problem~~ problems ~~and on information sent to the home location from at least one other remote client~~; and

sending in real time, from the home location to the remote clients, information for updating firewalls protecting the remote clients to account for the anomaly.

18. (currently amended) The method of claim 17 further comprising transmitting notice of the existence of the anomaly in real time from the home location to the remote client ~~location~~ locations.

19. (currently amended) The method of claim 17 further comprising notice of the existence of transmitting the anomaly in real time from the home location to other remote client locations that may communicate with the home location over the network.

20. (cancelled)

21. (currently amended) The method of claim 17 further comprising transmitting information from the home location to the remote client ~~location~~ locations to help the remote client location identify possible security problems.

22. (original) The method of claim 17 further comprising determining the existence of the anomaly based on at least information regarding previous anomalies.

23-27. (cancelled)

28. (currently amended) An apparatus comprising:

a server;

a first mechanism accessible by the server to determine an anomaly based on at least information from ~~a client~~ two or more clients regarding [[a]] possible security ~~problem~~ problems; ~~and on information sent to the home location from at least one other client; and~~

a second mechanism accessible by the server ~~and configured~~ to transmit notice of the anomaly in real time over a network to the clients; and

a third mechanism accessible by the server to update, in real time, firewalls protecting the clients to account for the anomaly.

29. (previously presented) The apparatus of claim 28 in which the first mechanism determines the anomaly based on at least information regarding previously determined anomalies.

30. (currently amended) A system comprising:

[[a]] two or more client ~~terminal~~ terminals;

a server;

for each of the client terminals,

a first client mechanism accessible by the client terminal to detect a possible security problem at the client terminal [[;]] ,

a second client mechanism accessible by the client terminal to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal [[;]] , and

a third client mechanism accessible by the client terminal to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems;

a first server mechanism accessible by the server to determine an anomaly based on at least information from ~~a client~~ two or more clients regarding [[a]] possible security ~~problem~~

problems; ~~and on information sent to the home location from at least one other client terminal;~~ ~~and~~

a second server mechanism accessible by the server to transmit notice of the anomaly in real time over the network to the client ~~terminal~~ terminals at which the possible security ~~problem~~ ~~is~~ problems are detected; and

a third server mechanism accessible by the server to update, in real time, firewalls protecting the clients to account for the anomaly.

31. (original) The system of claim 30 in which the first client mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem.

32. (original) The system of claim 30 in which the first server mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies.

33. (original) The system of claim 30 in which the second server mechanism is also configured to transmit notice of the anomaly in real time to other client locations that may communicate with the server over the network.

34. (currently amended) The system of claim 30 further comprising ~~a firewall~~ firewalls located between the client ~~terminal~~ terminals and the server and configured to act as an intermediary for information flowing between the client ~~terminal~~ terminals and the server.

35. (currently amended) The system of claim 34 in which ~~the firewall~~ at least one of the firewalls includes a corporate server.

36-38. (cancelled)

39. (cancelled)

40. (currently amended) A method comprising:

at a server, receiving from at least two remote clients indications of possible security problems at the clients; ~~and~~

determining in real time at the server an existence of an anomaly based on the indications of the possible security problems from the at least two remote ~~client locations~~ clients; and

sending in real time, from the server to the remote clients, information for updating firewalls protecting the remote clients to account for the anomaly.

41. (currently amended) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determining at the home location an anomaly based on the possible security problem by searching for particular information in the anomaly, the particular information including at least one of a network address previously noted as a security problem [[,]] and a particular query or command associated with a known intrusion pattern or technique~~, and a particular file name or file type associated with a known intrusion pattern or technique~~; and

transmitting notice of the anomaly in real time to the client location.

42. (currently amended) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location, including searching for an unexpected login; and

transmitting notice of the anomaly in real time to the client location.

43. (cancelled)

44. (cancelled)

45. (currently amended) The apparatus of claim 28, further comprising at least one of a human immune mechanism to collect information on users, a complexity theory mechanism to store and perform complex analysis of anomaly trends, ~~a statistics mechanism to compute and store records of anomalies,~~ and a fingerprinting mechanism to check and store names and addresses associated with security problems.

46. (previously presented) The apparatus of claim 28, further comprising a wide view mechanism to collect and maintain information regarding anomalies reported to the server by the clients.

47. (new) The apparatus of claim 28, further comprising a statistics mechanism to compute and store records of anomalies.

48. (new) The method of claim 40, further comprising at least one of collecting information on users by using a human immune mechanism, storing and performing complex analysis of anomaly trends by using a complexity theory mechanism, and checking and storing names and addresses associated with security problems by using a fingerprinting mechanism.

49. (new) The method of claim 40, further comprising computing and storing records of anomalies by using a statistics mechanism.

50. (new) The method of claim 41, further comprising updating, in real time, a firewall protecting the client location to account for the anomaly.

51. (new) The method of claim 42, further comprising updating, in real time, a firewall protecting the client location to account for the anomaly.

52. (new) The method of claim 42, in which searching for an unexpected login comprises searching for at least one of a login at an unexpected hour, a login from an unexpected location, and a login from an unexpected user.